| | |
|---|---|
| REGIONAL WIRELESS COOPERATIVE<br>POLICIES AND PROCEDURES | Regional Wireless Cooperative |
| | **No.**<br>**S-04.11** |
| **Subject:**<br>**Network Security Policy** | **Effective Date**<br>**9/22/11**<br>**(rev. 1/11/17)** |

## 1.0 Purpose

1.1. The purpose of this policy is to establish the security requirements for the RWC Network.

## 2.0 Owner

2.1. RWC Operations Working Group (OWG).

## 3.0 Applies To

3.1. Anyone with RWC system equipment access, including Members and approved service providers.

## 4.0 Background

4.1. The RWC system is a radio communications network comprised of computer systems, devices, and applications that directly support mission critical communications. It is important that the RWC system be protected from security-related risks that can cause network disruption or outage.

## 5.0 Policy Statement

5.1. Personnel that have access to the RWC infrastructure, consoles, IP logging recorders or network administration terminals shall at all times employ appropriate network security practices to protect the RWC from internal and external sources of harm that could potentially cause disruptions or failures in service. Examples include, but are not limited to, external connections, devices, access control, non-certified software and storage media.

## 6.0 Supporting Rules

6.1. Any computers that are used to connect to the RWC network, directly, will be protected for the purpose of supporting the RWC system. Support personnel are responsible for ensuring computers connected to the RWC Network have a current end point security solution.

6.2. Any media that is to be connected to RWC infrastructure, consoles, IP logging recorders or subscriber administrative terminals must first be scanned by an isolated computer that has an end point security solution.

6.3. The RWC Maintenance Manager(s), users and approved service providers are responsible for monitoring network incursions, which may be introduced by external media or non-certified software.

6.4. The Network Operations Manager shall have responsibility for ensuring that overall network security is consistent with current technology, and for ensuring that the RWC policies related to network security are followed.

6.5. RWC network users shall use due diligence in the protection of the RWC infrastructure, consoles, IP logging recorders, subscriber equipment and network resources.

6.5.1. Passwords must be protected and not shared with anyone without proper authorization.

6.5.2. User accounts will be created and managed by the RWC Network Operations Manager.

6.6. Any breaches in network security will immediately be reported to the Regional Operations Center (ROC) who shall take steps to minimize the danger to the operational capabilities of the RWC.

6.7. The Network Operations Manager will, as soon as possible, inform the OWG of a confirmed security breach, the current situational status, any known or potential impact to RWC operations and the steps taken to mitigate the impact of the breach.

## 7.0 Responsibilities

7.1. The Network Operations Manager is responsible for the following practices related to the RWC network security:

7.1.1. Update end point security solution software and server in compliance with Motorola network standards.

7.1.2. Monitor, identify, and maintain information related to RWC infrastructure and components regarding risks, threats, and vulnerabilities to the RWC.

7.1.3. Develop plans for minimizing or eliminating security-related problems, and any actions necessary for the implementation of the plans.

7.1.4. Use the appropriate supporting organizations or approved contractors as required to maintain adherence to network security policies.

7.1.5. Provide reports to the OWG on the status of network security, potential threats and risks, and actions involved in protecting RWC.

7.2. Member agencies are responsible for ensuring approved users and service providers adhere to this policy.

7.3. Any security breaches must be reported to the Networks Operations Manager as soon as possible.

## 8.0 Conditions for Exemption or Waiver

8.1. None.

## 9.0 Applicable Policies and/or Procedures

9.1. As listed at www.rwcaz.org